APPENDIX 2

Dartford Borough Council

Information Security Policy

I T Delivery
May 2006
# Contents

1. **Introduction** .................................................................................................................. 4
   1.1. Background ................................................................................................................. 4
   1.2. Information Security .................................................................................................. 4
   1.3. Purpose of the Policy document ............................................................................... 4
   1.4. Scope ......................................................................................................................... 5
   1.5. Objectives ................................................................................................................. 5
   1.6. Document Control ..................................................................................................... 6

2. **Roles and Responsibilities** ............................................................................................. 7
   2.1. Managing Director ................................................................................................... 7
   2.2. Management Team ................................................................................................... 7
   2.3. IT Manager (Delivery) ............................................................................................... 7
   2.4. System owners (see Appendix E) ............................................................................. 7
   2.5. Managers ................................................................................................................... 7
   2.6. All Users of IT systems – Members, staff and other authorised people .................... 7
   2.7. IT development, support and maintenance staff ......................................................... 8
   2.7. Monitoring compliance ............................................................................................. 8

3. **Legal Requirements** ..................................................................................................... 9
   3.1. The Data Protection Act 1998 ................................................................................... 9
   3.2. The Copyright, Designs and Patents Act 1988 ........................................................... 9
   3.3. The Computer Misuse Act 1990 ................................................................................. 10
   3.5. Freedom of Information Act 2000 (FOI) ................................................................ 11

4. **Education and awareness** ............................................................................................. 12
   4.1. Job descriptions .......................................................................................................... 12
   4.2. Recruitment ............................................................................................................... 12
   4.3. Training ...................................................................................................................... 12
   4.4. Confidentiality ............................................................................................................ 12
5. Reporting security incidents

5.1. Who to report an incident to?

5.2. IT Helpdesk and IT Manager (Delivery)

5.3. Confidentiality

5.4. Disciplinary proceedings

6. Policy Statements

6.1. Identification and control of assets

6.2. Procurement

6.3. Inventory

6.4. Change Management

6.5. Physical and environment security

6.6. The computer room and associated areas

6.7. Information security

6.8. Equipment security

6.9. Off-site considerations

6.10. Personal computers and terminals

6.11. Network

6.12. The Internet and Internet email

6.13. Access to systems


6.15. Back ups

6.16. Business Continuity Planning

7 Audit and control
1. Introduction

1.1. Background

Dartford Borough Council has a large investment in Information Technology (IT) which is an essential resource that is used either directly or indirectly in the delivery of all of the Council's functions. It is vital therefore that IT is protected from any form of disruption or loss of service and it is essential that the availability, integrity and confidentiality of the IT systems and data are maintained to the highest standards.

The Council is the custodian of large amounts of electronically stored information, much of it of a personal and sensitive nature. In order to carry out the business of the Council, this information must be accessed by computer application systems and transmitted across communications networks operated by the council.

In addition, electronic information is also sent and received via email and the Internet for which specific guidance already exists in the Internet and Email Policy (reproduced in Appendix F) to supplement the general guidance within this document.

Information is a valuable asset which must be protected to ensure the effective and accurate operation of the computer systems on which the Council relies. There are legislative and regulative obligations placed on the Council in respect of the confidentiality of much of this information which must be observed. Failure to protect information could jeopardise the ability of the Council to provide efficient, cost-effective services to the general public.

It is essential, therefore, that Information Security controls are established to prevent information being accidentally or maliciously misused, corrupted, lost or destroyed.

1.2. Information Security

The purpose of Information Security is to protect information in the following key areas:

Confidentiality ensuring that information is protected against unauthorised access or disclosure.

Integrity ensuring that information is accurate, complete and free from corruption.

Availability ensuring that information is available when it is required.

Non-Repudiation ensuring the ability to prove the origin of information or disprove a denial of receipt.

1.3. Purpose of the Policy document

The purpose of this Information Security Policy document is to define the stance of Dartford Borough Council with regard to certain aspects of Information Security which are described in the body of the document.

The Policy document is a framework for the establishment of standards and procedures for Information Security Management and is based on the guidance contained in BS7799, a code of practice for Information Security Management.
The Policy Document has a number of appendices which give practical advice and guidance to users in specific areas of Information Security. Some of these appendices have been made available in the form of Information Leaflets.

1.4. **Scope**

The Information Security Policy applies to all Council locations and elsewhere where Council business is undertaken, and applies to all staff, councillors, agents, contractors and volunteers working for, or on behalf of, the Council.

The generic terms user and users are used within this policy to refer any of above.

For the purposes of this document, the term ‘information’ covers:

- data, software and images stored on and accessed by computer systems,
- data, software and images transmitted electronically across networks, both internal and external,
- data, software and images stored on magnetic media.

The guidance within the Policy document also applies, where relevant, to other kinds of information which may be printed, sent or received by fax and stored on film or microfiche.

Note: The Council has a specific code of practice for the use of CCTV equipment.

The guidance will also apply to certain manual records covered under the Data Protection Act 1998. These will include records (e.g. application forms) relating to computerised information and may include manual filing systems where they are structured to enable easy reference to personal information e.g. a personnel filing system. If in doubt please seek advice from your line manager.

**This Information Security Policy is a Council policy and infringements may result in formal action against those found to have breached it.**

1.5. **Objectives**

The objectives of the Council’s Information Security Policy are:

- To ensure that all users of Council information and Information Technology systems are aware of the need for Information Security and have an appreciation of their responsibilities.
- To define broad organisational roles and responsibilities.
- To provide a framework which gives guidance on a number of aspects relating to information security, as defined in the policy document.
1.6. Document Control

This document has been produced, and will be updated and maintained by IT Services and, except for minor factual updates, will be approved by Management Team. The Policy will be published on the Council’s Intranet and printed copies will be available to staff, elected Members, contractors, agency staff and volunteers on request.
2. Roles and Responsibilities

2.1. Managing Director

The Managing Director has overall responsibility for the development and implementation of this Policy.

2.2. Management Team

The Management Team will direct the broad strategy and approve the Policy and any changes to it other than those of a minor factual nature.

2.3. IT Manager (Delivery)

The IT Manager (Delivery) will, subject to approval by Management Team, develop, publish and maintain Dartford Borough Council's Information Security Policy. These activities will include developing, reviewing and auditing procedures compliant with this Security Policy.

2.4. System owners (see Appendix E)

For major IT applications, the role of System Owner has been identified. The System Owner, who should be a system user of appropriate seniority, must ensure that:

- Access controls are in place which are appropriate to the sensitivity of the information used by the system;
- Procedures are in place to ensure that regular back-ups of both software and data are taken, and copies are stored in a secure remote location;
- The major risks which may threaten the security of the information are identified and, where possible, mitigated;
- Changes to the system are authorised and made in a controlled and effective manner.
- Instances of misuse or abuse of the system are reported as per section 5.0.

Note that IT Services are responsible for procuring new software items, for managing and controlling software licences, for providing a secure area for the storage of definitive versions of software, for the distribution and implementation of new and amended software versions, and for the automated back-ups of networked systems.

2.5. Managers

Managers must ensure that they, their staff and any agency staff, volunteers and contractors are aware of and comply with the Information Security Policy, and that they are kept informed of any updates.

2.6. All Users of IT systems – Members, staff and other authorised people

Users of computer systems must ensure that they comply with the guidance contained within the Information Security Policy, and report any actual or suspected breaches via
the appropriate channel. See Section 5 for further guidance on reporting security incidents and see Appendices A – C in particular for detailed guidance on passwords, use of PCs and control of viruses.

2.7. **IT development, support and maintenance staff**

Staff working within IT Delivery are responsible for the support, maintenance and development of computer systems. IT Delivery staff may therefore have privileged access to computer systems and to personal and confidential information in order to carry out their normal responsibilities. They must ensure that they are aware of and comply with the information security provisions relating to each computer system as well as this general policy guidance.

2.7. **Monitoring compliance**

The diverse nature of this policy means that responsibility for monitoring its compliance will be shared between senior management, IT Manager (Delivery), system owners and managers depending on the facet of the policy being considered.
3. **Legal Requirements**

The Council will observe all laws and regulations which apply to Information and computer systems. These include:

3.1. **The Data Protection Act 1998**

The Act seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information.

The Act gives individuals certain rights regarding information held about them e.g. to ask for a copy of the data held about them. It places obligations on those who process information (data controllers) while giving rights to those who are the subject of that data (data subjects). Personal information covers both facts and opinions about the individual. The Council is a data controller and is required to register its uses of the processing of personal data and to comply with the data protection principles to ensure (inter alia) that:

- Data is obtained and processed fairly and lawfully;
- Data held will be accurate and not excessive for the purpose required;
- Data will not be retained for longer than is necessary;
- Data is protected from accidental or unauthorised loss or destruction;

Guidance on data protection is viewable on the intranet. The guidance explains what the Council’s responsibilities are when dealing with subject access requests etc.

If you require any guidance on the Data Protection Act please contact the Council's Data Protection Officer, Head of Legal Services, on ext 3634 or visit the Information Commissioner’s website http://www.informationcommissioner.gov.uk/eventual.aspx?id=34

3.2. **The Copyright, Designs and Patents Act 1988**

This Act makes it illegal to copy any piece of software without the owner’s permission. Most proprietary software is supplied under a licence agreement which limits the use of the software to specified platforms and numbers of users. Copying of the software will normally be restricted to the creation of back-ups.

To comply with the law:

- all purchased software must have appropriate licence agreements;
- purchased software can only be used on platforms covered by the licence;
- definitive versions of proprietary software and the licence agreements must be stored in a secure place; IT Services are responsible for storing software and licences.

Criminal prosecutions may result from infringements of copyright law.
3.3. **The Computer Misuse Act 1990**

This Act recognises that certain activities constitute computer crime, and provides legal redress against offenders.

Broadly speaking, computer misuse is categorised as:

- attempted unauthorised access to a computer system;
- attempted unauthorised access to information;
- access with a view to personal gain.

Users must report any instances of potential or suspected misuse of computers via the mechanism described in Section 5.


The Regulation of Investigatory Powers Act 2000 (RIPA) governs the interception of communications, covert surveillance operations and access to encrypted data.

A Code of Practice on the Use of Personal Data in Employer/Employee Relationships has been developed which addresses the impact of the Data Protection Act 1998 on the monitoring by employers of telephone calls, e-mails and Internet access involving their employees. The Council is authorised in relation to its internal communications network to monitor or record all communications transmitted over its system without consent for the following purposes:

(a) establishing the existence of facts;

(b) ascertaining compliance with regulatory or self-regulatory practices or procedures;

(c) ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system;

(d) preventing or detecting crime;

(e) investigating or detecting unauthorised use of the Council's telecoms system;

(f) ensuring the effect of the proper operation of the system.

The Council may monitor (but not record) communications to check whether or not communications are relevant to the Council.

The Council is required to "make all reasonable efforts to inform those people who use the Council's telecom systems that interceptions may take place". Dartford Borough Council through this *Information Security Policy*, informs all users of Dartford Borough Council systems of its intention to access, record and monitor information in order to ensure the appropriateness of their use of information and activities performed through information systems, facilities, and processes established for Dartford Borough Council business purposes. If you require any guidance on RIPA please contact the Council's Head of Legal Services, on ext 3634.
3.5. **Freedom of Information Act 2000 (FOI)**

The Freedom of Information Act 2000 (FOI) creates a general right of access to information held by public bodies (including local authorities) but subject to wide-ranging exceptions.

The general principle is that any person making a request for information to a public authority is entitled to be informed whether the public authority holds information of the description specified in the request, and, if yes, to have that information communicated to him/her.

A Manual is viewable on the intranet giving guidance and assistance in dealing with requests under the FOI Act. It explains what the Council's responsibilities are when answering requests for information held by the Council.


For further guidance on the Freedom of Information Act contact Head of Legal Services, on ext 3634.
4 Education and awareness

4.1. Job descriptions

The Council will ensure that:

Where appropriate, specific security roles and responsibilities are defined and documented in job descriptions.

Individuals who have a responsibility for the protection of information assets are aware of their specific responsibilities.

All Council employees are aware of, and have access to information relating to security procedures.

4.2. Recruitment

Appropriate security screening measures may be taken when dealing with applications for employment, especially when the job involves dealing with information which the recruiting officer considers to be sensitive. These screening procedures may also be invoked if employees change roles within the organisation, and their new role involves dealing with information of a sensitive nature.

4.3. Training

The Council will ensure that all users of IT systems are aware of security requirements and procedures before being allowed access, and that training is available on the correct and secure use of IT facilities. This is the responsibility of Line Managers.

4.4. Confidentiality

The Council’s standard contract of employment contains a section setting out that it is the duty of staff not to disclose to a third party or otherwise use any of the Council’s confidential information either during or after the termination of employment with the Council.

Agency, contract staff and contractors must abide by the relevant conditions of contract with regard to security matters, and may be required to sign confidentiality and non-disclosure undertakings prior to being allowed access to IT facilities, as may volunteers. This is the responsibility of the relevant Manager.
5. Reporting security incidents

It is the responsibility of all users to report any observed or suspected security weaknesses in IT systems or services. The Council will maintain various methods for users to report actual or suspected breaches in security procedures, as set out below.

Users must not attempt to test or prove suspected weaknesses themselves. Such action may be misconstrued as an attempted breach of security and investigated and dealt with in accordance with the Council’s Disciplinary Procedure or Member Code of Conduct, as appropriate. For external users under contract to the Council, such action could be considered to be breach of contract or investigated under the provisions of the Computer Misuse Act 1990.

The Council’s mail scanning or internet monitoring systems automatically flag hundreds of items and events instances daily in an attempt to balance protection for the network and the individual users with the avoidance of delay. These will not be treated automatically as a security incident unless subsequent inspection by IT Staff reveals the need for this.

5.1. Who to report an incident to?

Where fraud and/or money laundering is suspected this should be reported in the first instance to the Managing Director, the Money Laundering Reporting Officer, who is the Head of Finance and Resources, and the Monitoring Officer. The whistleblowing procedure may be used for this purpose.

In other cases, staff should normally report actual or suspected breaches in security procedures via their Line Management. If this is not possible or appropriate it should be reported to either the reporter’s Director or the Audit Manager.

Members should report actual or suspected breaches of the Policy to the Monitoring Officer. The Policy has been drawn to Members’ attention by virtue of its inclusion on the Agenda of Audit & Standards Board and Cabinet and by letter.

The Policy will form part of the standard contract terms and conditions, or other agreement, for external users working on behalf of the Council. Contractors or other external users are directed to their Client Monitoring Officer.

5.2. IT Helpdesk and IT Manager (Delivery)

Users should report or discuss security matters of a general systems nature rather than individual behaviour with IT Manager (Delivery) x3130) or the IT Help Desk. X 3850

The Help Desk record all incident reports, and will maintain an incident category for security incidents. These incidents reports will be passed to the IT Manager (Delivery) so that the appropriate action is taken. The IT Manager (Delivery) will ensure that steps are taken to test suspected weaknesses, and to rectify breaches.

Issues relating to viruses should be reported to IT Help Desk.

5.3. Confidentiality

The Council’s Whistleblowing Policy provides guidance as to how employees can raise a concern without fear of recrimination. These procedures, which are referred to in both
the Policy on Anti-fraud and Corruption and the Code of Conduct, can be used when necessary by employees to report security matters. The Whistleblowing Policy details points of contact.

5.4. Disciplinary proceedings

This Information Security Policy is a Council policy and infringements may result in the invocation of the Council’s Disciplinary Procedure (in respect of staff) or Member Code of Conduct (in respect of Members).
6. **Policy Statements**

6.1. **Identification and control of assets**

The Council will identify all assets which are important for the provision of IT systems and services. Assets can be characterised as:

- **Information** databases and files, documentation and manuals, procedures and plans etc.
- **Software** applications, operating systems, tools and utilities which may be developed in-house, or bought-in packages.
- **Physical** computer and network hardware, ancillary equipment, furniture, telephones etc.

IT Services will maintain inventories of all computer hardware and software.

6.2. **Procurement**

All requests for new equipment and software must be agreed by the IT Delivery Manager to ensure that what is bought for use on the Council’s network is both compatible and appropriate in terms of the requirements of this Policy.

6.3. **Inventory**

Assets which are deemed to be an important component of computer systems or service delivery such as base units and monitors will be physically identified and their existence will be recorded in the IT Inventory. This is used as a key component of the IT helpdesk system, provide information for the insurance policy and a means of recharging IT costs. IT Delivery are responsible for procuring, identifying and recording assets of this nature, and for maintaining the IT Inventory and Section Managers should inform IT Delivery of any changes affecting the IT Inventory. IT Delivery will also maintain an inventory of the Council’s software and software licenses. The IT Inventory forms part of the Council's general inventory.

6.4. **Change Management**

All changes to physical and software assets must be made under the control of IT Services. In conjunction with IT Delivery, Managers must ensure that any changes made to the assets for which they are responsible are assessed as to whether there is any impact on security controls.

6.5. **Physical and environment security**

The Council will ensure that the following general controls on physical access and security are maintained.

- Council offices and areas accessible only by staff, Members and authorised visitors will be protected by appropriate security controls from areas of Council premises accessible by the general public.
- The date and time of entry and departure of all visitors to the Civic Centre should normally be recorded.
• Wherever possible visitors to Council premises will be supervised.

• All staff and visitors will be required to wear identification badges.

The Senior Civic Centre Services Officer will work with IT Manager (Delivery) to ensure that the computer room and other locations used to house sensitive IT assets are protected from unauthorised access and that suitable services and environmental facilities are provided.

6.6. The computer room and associated areas.

IT Delivery will ensure that the computer room and other locations used to house sensitive IT assets are protected from unauthorised access by appropriate locks and/or authentication controls.

6.7. Information security

Users must ensure that information considered to be sensitive to which they have access, such as passwords, computer discs etc., are locked away when offices are unattended.

Section Managers must ensure that suitable facilities are provided for the storage of sensitive information. The nature of the information will determine what is suitable. This could include a locked desk drawer, locked cupboard or in some instances a safe.

Unwanted equipment and media must be returned to IT Services. The IT Manager (Delivery) will decide whether it is to be disposed of and in any case will ensure the removal or destruction of information and licensed software prior to reuse of the equipment or as part of the disposal.

6.8. Equipment security

IT Delivery staff and Section Managers must ensure that appropriate security measures are considered when positioning, installing and connecting new or relocated equipment. These measures include:

• prevention of unauthorised access, either directly or remotely;

• prevention of damage, interference or destruction, either accidentally or deliberately;

• prevention of theft;

• prevention of unauthorised copying, modification and deletion of information and software.

Please contact the IT Manager (Delivery) if advice and guidance is required.

6.9. Off-site considerations

Management authorisation must be acquired prior to removing Council IT equipment off-site. It is the responsibility of the user removing equipment to ensure that appropriate security controls exist at the off-site location, and that sensible measures are taken to protect equipment whilst in transit.
Relevant Managers must maintain a record of either the current location of portable IT equipment, or the person responsible for it, and must be aware of any provisions regarding the insurance of items in transit or located off-site. Subject to normal domestic security arrangements being applied, items held at home are covered by insurance but items are NOT covered if left in an unattended vehicle.

Users of Council computer equipment away from Council office/s are responsible for ensuring that all relevant security controls are applied.

6.10. Personal computers and terminals

The Council will provide Members and staff with appropriate computer equipment to carry out their Council function, and it is the duty of those individuals to ensure that basic security controls are applied to personal computers, printers and other IT related equipment used by them.

These basic controls include:

- Ensuring that the correct start-up and close-down procedures are carried out at the beginning and the end of working periods. For reasons of safety as well as security, PCs should be switched off at the end of the day and not left on overnight.

- Ensuring that personal computers are not left logged-in while unattended. A password protected screen saver should be activated during any absences. When leaving for the day, you should normally terminate all applications and log out of the PC.

- Ensuring that no unauthorised software is introduced onto personal computers. IT Services are responsible for the installation of all software.

- Ensuring that password controls are understood and adhered to - this includes the procedures for changing and storing passwords.

- Taking all reasonable precautions against theft and unauthorised use when using the Council’s portable and laptop computers.

More detailed guidance in relation to Passwords, PCs and Viruses is provided in Appendices A–C.

6.11. Network

IT Delivery staff are responsible for the installation, maintenance and management of the Council’s internal data networks, and for installing, maintaining and managing links to external data networks such as those owned by other organisations, and the internet.

IT Services are responsible for ensuring that the network is protected from:

- unauthorised access to information and systems;
- interception of data;
- exposure and modification of data;
• hacking, abuse and misuse.

IT Services are responsible for the introduction of measures to protect the integrity of the network and the information flowing across it.

6.12. The Internet and Internet email

Members and Staff must ensure they comply with the Council’s Internet Use Policy (where applicable) and Email Protocol which has been previously issued to all staff and Members but for completeness is also attached as Appendix F.

IT Delivery will monitor use of the Internet and will ensure that suitable security is maintained.

6.13. Access to systems

The Council’s computer systems and equipment must only be used by authorised personnel and only in pursuance of their duties. Any departure from this should be agreed with the System Owner (see Appendix E). Additionally, restricted personal use of the internet and email is permitted as set out in the internet usage policy appendix F and the email protocol appendix G.

Staff who require access to the Council’s computer systems must first gain authorisation from their Manager who must follow a user registration process. Staff must make themselves familiar with the relevant log-on, log-off and password control procedures.

Members and external users will be given access to those systems necessary to enable them to perform their function.


Significant changes made to the Council’s computer systems must be assessed for their security implications by the System Owner, referring to the IT Manager (Delivery) when necessary.

IT Delivery staff are responsible for the development and assisting with the procurement of new computer systems, and must ensure that appropriate Information Security controls are included in system design and specifications.

More detailed guidance on this subject is provided in Appendix D. Further advice can also be obtained from the IT Manager (Delivery).

6.15. Back ups

Security copies (back ups) of systems operating on the network will be taken on behalf of users by IT Services at predetermined frequencies. These are automatically scheduled to be taken at regular intervals dependant upon the importance and quantity of the data concerned.

The general approach for the backups is that on at least a weekly basis a snapshot of the system is taken (and at least 3 generations are retained) and on a daily basis each active system (e.g. Council Tax) is secured. The nature of the system determines the period for which these are kept, typically 2 weeks.
The most recent archives are stored in the fire safes while at the Civic Centre but are regularly sent off-site for disaster recovery purposes.

No Information stored on the C: drive of a PC is backed up and users should ensure that all important information is stored on the network (S: or H: drives) or secured to some removable storage.

All backups aim to enable both a full system recovery and the specific reinstatement of parts of the system. However the differing natures of the systems means that the ease of recovery of parts of some of the system is not always straightforward.

6.16. Business Continuity Planning

Council Services are responsible for maintaining the continuity of their own business processes in the event of a major incident.

IT Services are responsible for the recovery of IT systems to support Council Services and will maintain a disaster recovery plan.
7 Audit and control

The Information Security Policy has been authorised by the Management Team, and its contents will be kept under constant review by the IT Manager (Delivery). Any changes required that are other than of a minor factual nature must be authorised by the Management Team.

Empowerment to carry out spot checks and audits of equipment, software, users and procedures to ensure conformance to the Policy will be shared between senior management, IT Manager (Delivery), Internal Audit, system owners and managers depending on the facet of the policy being considered.